REMARKS/ARGUMENTS

Claim Amendments

The Applicant has amended claims 1, 7 and 11. Applicant respectfully submits no new matter has been added. Accordingly, claims 1-4 and 7-17 are pending in the application. Favorable reconsideration of the application is respectfully requested in view of the foregoing amendments and the following remarks.

Claim Rejections – 35 U.S.C. § 103 (a)

Claims 1-4 and 7-17 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Anton et al (US Patent 7,185,360) in view of Inoue, et al. (US Patent 6,163,843). The Applicant respectfully traverses this rejection.

The present invention claims the use of an identifier for a user by first and second networks towards an application, independent of the networks, wherein the identifier is generated by the first network and is then requested by the second network to provide access by the user to the second network. The Applicant respectfully asserts that neither Anton nor Inoue, individually or in combination, discloses the limitations or elements of the independent claims.

Previously, (Office Action dated 16 April 2009, p.5, second paragraph) the Examiner first network is regarded a being provided by access points/further networks that are comparable to the second network 129, where the mobile device can access the Internet via these networks. The identifier is not generated and used by the first network towards the authorized web page 133 but rather generated by authentication server 131. The second network 129 does not request an identifier from the first network and does not receive this identifier from the first network in order to use this identifier towards the application.

Next, (Office Action dated 16 April 2009, p. 4, last paragraph – p.5, first paragraph) the first network is regarded as the authentication server 137/gate keeper 135 which generates an identifier (cf. Office Action above; Anton: col. 10, l. 30-35). Thus the second network still corresponds to network 129. Using this interpretation, the first network does not use this identifier towards the application, since the web page cannot

be accessed through the authentication server. Further, the second network does not request an identifier from the authentication server.

Even when interpreting the first network to be constituted by the servers and a further access point/network, the identifier used by this further access point/network is not the same as the identifier used by the network 129 as the identifier is dependent on the access point (D1: col. 5, l. 31-34, col. 9, l. 54-57, col. 10, l. 34-36). Again, network 129 does not request an identifier from the authentication server 131.

Regardless of which interpretation is used, the first network and the second network in Anton do not use the same identifier towards the application. Further, the second network does not request the identifier from the first network.

Inoue does not disclose using the same identifier towards the application by the first and second networks. Further, Inoue does not disclose the second network requesting an identifier from the first network to identify the user towards the application.

Inoue discloses a method of rerouting data from a home network to a foreign network in which a mobile computer is currently located. Granting the mobile computer access to the internet for communicating with the home network is based on the foreign network generating key information for the mobile computer (Inoue col. 10, l. 28-35, col. 11, l. 20-40). In order to then enable the rerouting of the data from the internet via the home network, the mobile computer sends a registration message to the home network and receives a registration response (Inoue col. 11, l. 61-67). Thus, the mobile computer has already been granted access to transmit data outside the foreign network before sending a registration message to the home network. Therefore, the mobile computer can already access the internet using his new authentication data. Secondly, the authentication data generated based on the key information of the particular network and used by the mobile computer to identify him towards the internet are different for the home network and the foreign network (Inoue col. 11, l. 50, 51, col. 12, l. 24-35). Thus, the foreign network requests the "wrong" identification from the home network in order to identify the mobile computer towards the internet. The Applicant respectfully submits that amended claim 1 and the analogous independent claims 7 and 11 are allowable over the cited art, Anton and Inouye, individually or in combination.

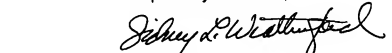
Claims 2-4, 8-10 and 12-17 depend from amended claims 1, 7 and 11 respectively and recite further limitations in combination with the novel elements of these independent claims. Therefore, the allowance of claims 2-4, 8-10 and 12-17 is respectfully requested.

CONCLUSION

In view of the foregoing remarks, the Applicant believes all of the claims currently pending in the Application to be in a condition for allowance. The Applicant, therefore, respectfully requests that the Examiner withdraw all rejections and issue a Notice of Allowance for all pending claims.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,



By Sidney L. Weatherford
Registration No. 45,602

Date: October 16, 2009

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024

(972) 583-8656
sidney.weatherford@ericsson.com